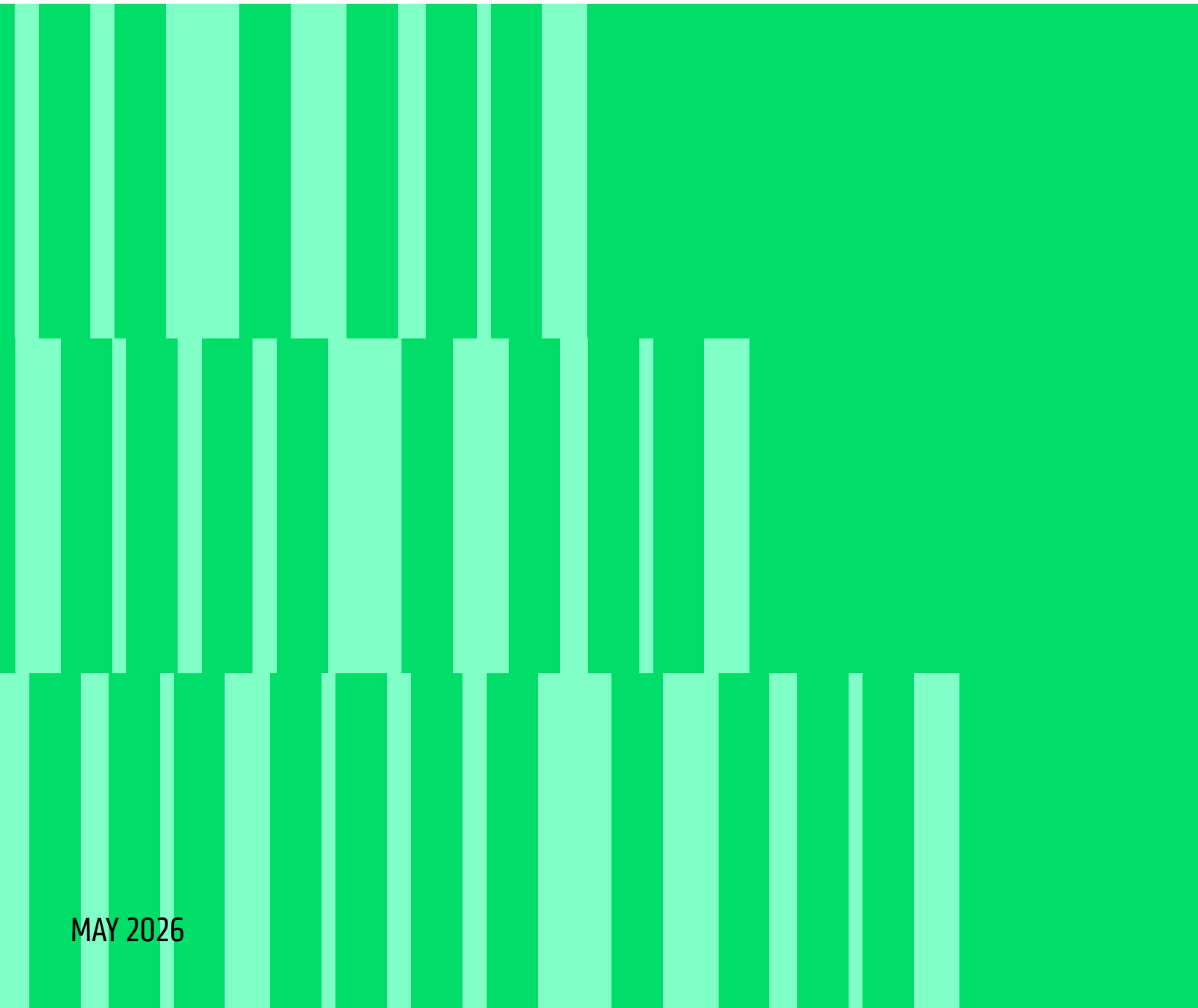
COHESITY

# CYBER RESILIENCE REPORT

## Risk-Ready or Risk-Exposed: The Cyber Resilience Divide in Midsize Organizations



MAY 2026

Everyone talks about detecting and preventing cyberattacks, yet the headlines tell a different story. Prevention and detection alone are no longer enough. Even the most advanced organizations are suffering crippling disruptions that ripple from IT operations to the boardroom—and beyond.

To understand why, and what separates resilient organizations from those still struggling, Cohesity surveyed 3,200 IT and Security Operations decision-makers across 11 countries. Among those were nearly 1,000 participants from midsize organizations. Their responses reveal a widening resilience divide between risk-ready organizations that can recover quickly and confidently, and their risk-exposed peers that remain vulnerable to prolonged disruption and downstream financial damage.

Our research examines the real-world impacts of material cyberattacks, how midsize organizations self-assessed their cyber resilience against best practices, and the steps they took to detect, respond to, and recover from these incidents. It also highlights what they learned, and how they're turning to AI and automation to accelerate resilience and close the divide.

## MATERIAL CYBERATTACKS:
## THE NEW REALITY OF MODERN BUSINESS

Cyber incidents are not created equal. Many organizations manage routine phishing attempts, malware probes, or system outages on a near-daily basis. But material cyberattacks are different. Our survey defined a material cyberattack as an incident that caused measurable financial, reputational, operational, or customer churn impact.

### THESE HIGH-IMPACT ATTACKS ARE NO LONGER ISOLATED EVENTS FOR MIDSIZE ORGANIZATIONS.

**75%**

of respondents have experienced at least one material cyberattack.

**55%**

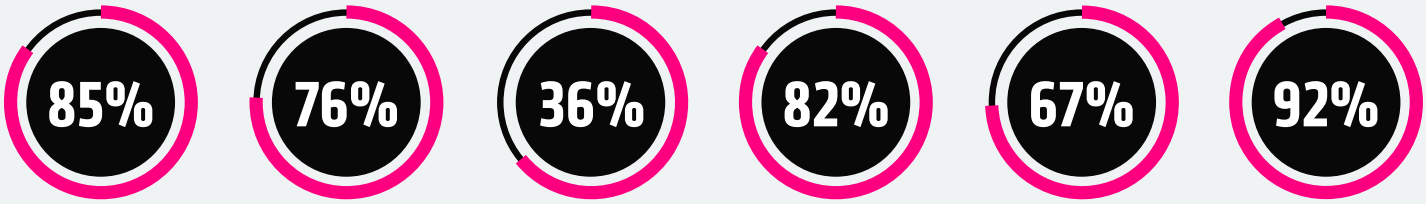
experienced one within the past 12 months.

**25%**

endured multiple incidents during the 12-month period.

# THE ACTUAL COST OF MATERIAL CYBERATTACKS

## FINANCIAL AND REGULATORY PRESSURES ALSO ECHOED ACROSS THE MIDSIZE ORGANIZATIONS WE SURVEYED:




85% reported revenue loss

76% of publicly listed organizations reported revising financial guidance[1]

36% lost customers

82% paid a ransom—averaging USD 1.3 million per incident

67% of privately held organizations reallocated budget away from growth initiatives

92% faced legal or regulatory consequences, including regulatory fines (46%) and lawsuits or class action litigation (33%)

[1] While relatively few public companies have formally disclosed earnings revisions after a cyber incident, these findings suggest that the financial and operational effects extend well beyond what public filings reveal.

## CONFIDENCE IN THE FACE OF CONSEQUENCE

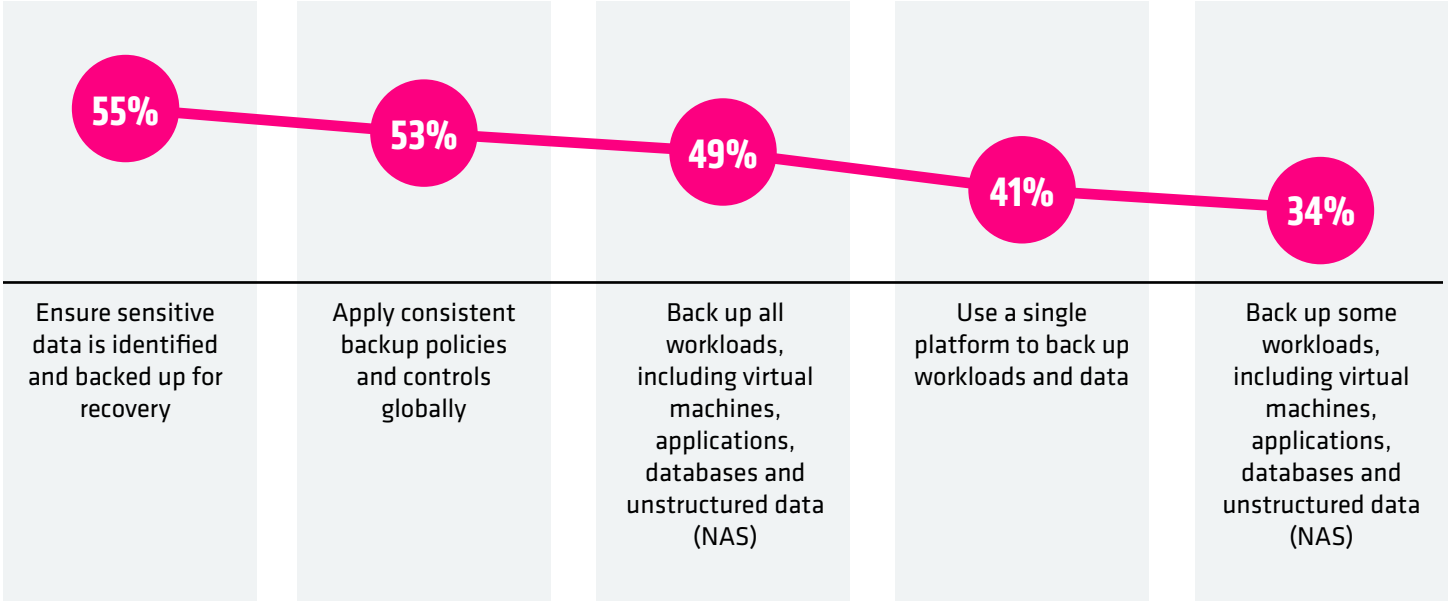
Given the scale of financial and operational fallout revealed in our research, one might expect widespread concern about organizational resilience. However, many respondents (47%) expressed complete confidence that their cyber-resilience strategy could withstand today's threats. This level of confidence stands in sharp contrast to the significant material impacts many of these same organizations have sustained.

## WHAT ORGANIZATIONS ARE (AND AREN'T) DOING

We wanted to look beneath the surface and discover where resilience gaps exist. To do that, we asked respondents to describe their approach to some of the key practices and capabilities associated with five core dimensions of cyber resilience: **data protection, data recovery, threat detection and investigation, application resilience,** and **data risk posture optimization.**

## DATA PROTECTION REMAINS FRAGMENTED ACROSS HYBRID AND MULTICLOUD ENVIRONMENTS

What does your organization do to protect all data across hybrid and/or multi-cloud environments?




Just over half of midsize organizations ensure sensitive data is identified and backed up for recovery. Roughly the same share applies consistent backup policies and controls globally. Fewer than half back up all workloads or use a single platform to protect workloads and data. A third back up only selected workloads. This fragmentation limits visibility and consistency across environments. Mature cyber resilience depends on unifying backup and recovery within a single intelligent platform secured by Zero Trust principles.

## DATA RECOVERABILITY MEASURES ARE COMMON BUT MATURITY VARIES

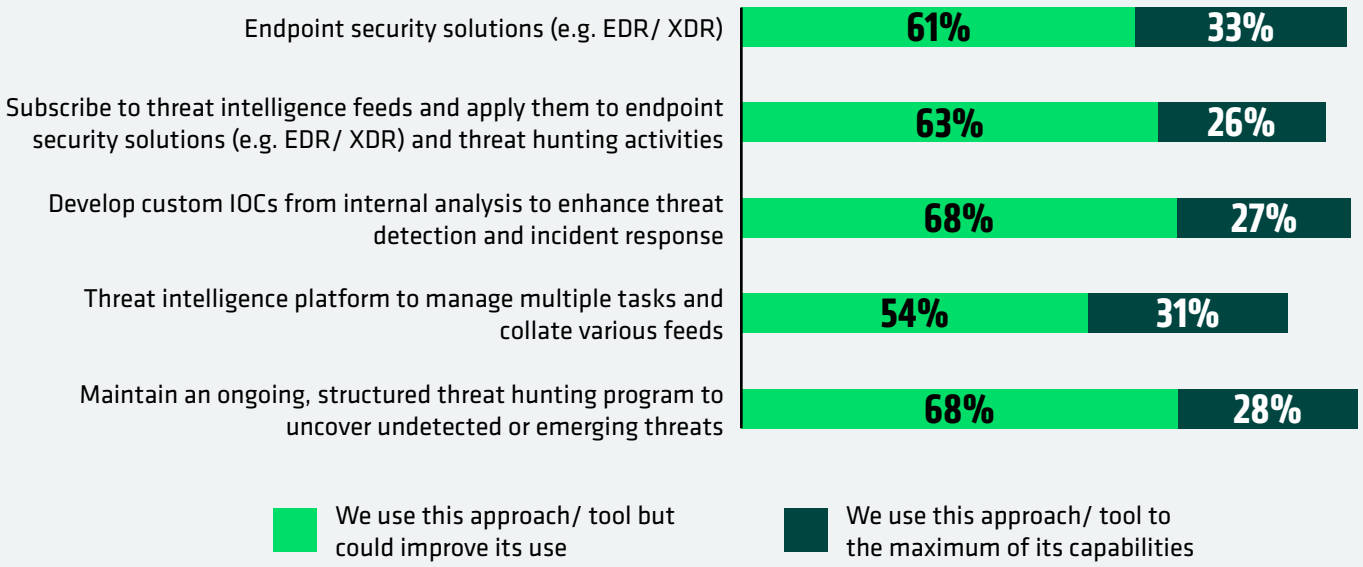
What does your organization do to ensure that its data is always recoverable?

| | |
|---|---|
| **60%** | Require additional authorization on high-risk admin tasks associated with backup and recovery solutions |
| **53%** | Multi-factor authetication on our backup solution |
| **47%** | Follow the "3-2-1 backup rule" (three copies of data, stored on two different media types, with one copy kept off-site) |
| **42%** | Protect critical data with immutability |
| **38%** | Least privilege access rights on backed up workloads |

Many midsize organizations have strengthened access controls around backup environments, with more than half requiring additional admin authorization for high-risk tasks. Around half enforce multifactor authentication and close to half follow the 3-2-1 backup rule. Fewer protect critical data with immutability or apply least-privilege access rights. These gaps make full recovery less certain. Mature cyber resilience depends on verified, isolated, and tamper-proof recovery copies.

## THREAT DETECTION AND INVESTIGATION TOOLS ARE UNDERUTILIZED

To what extent does your organization use each of the following methods or tools to detect and investigate threats?




Threat detection and investigation tools are widely deployed but often underutilized. Most midsize organizations use endpoint security, threat intelligence feeds, custom IOCs, threat intelligence platforms, and structured threat hunting programs, yet only a minority leverages these tools to their full potential. Mature cyber resilience depends on integrating these tools into a continuous intelligence loop that improves visibility, detection, and response.

## INCOMPLETE RESILIENCE MEASURES RAISE REINFECTION RISK

What does/ would your organization do to ensure application resilience against cyberattacks?

**57%** Identify and remediate security control gaps before restoring systems to production

**60%** Conduct annual end-to-end simulated rehearsals including a cross functional team of technical, legal, strategic, executive and communications stakeholders

**56%** Use online, vaulted repository of critical systems and information to support incident response and recovery

**47%** Use an isolated environment for incident investigation, remediation and secure recovery

**33%** Immutability for all backup data

Midsize organizations are advancing their approach to application resilience, but gaps remain. A majority identify security control gaps before restoring systems. A comparable proportion maintain online vaulted repositories. More than half also conduct annual recovery rehearsals. Fewer use isolated environments for secure investigation and recovery. An even smaller percentage applies immutability across all backup data. These gaps leave recovery processes vulnerable to reinfection or data loss. Mature cyber resilience pairs preparation with secure, verifiable recovery zones.

## DATA CLASSIFICATION GAINS TRACTION AS RISK USE EXPANDS

How does your organization use data discovery and classification approaches/ tools to minimise data risk exposure across its entire data estate?


Identify and resolve backup privacy and security violations for compliance

Use backup data classification to determine compliance obligations for impacted data

Define and understand cyberattack materiality before an incident occurs

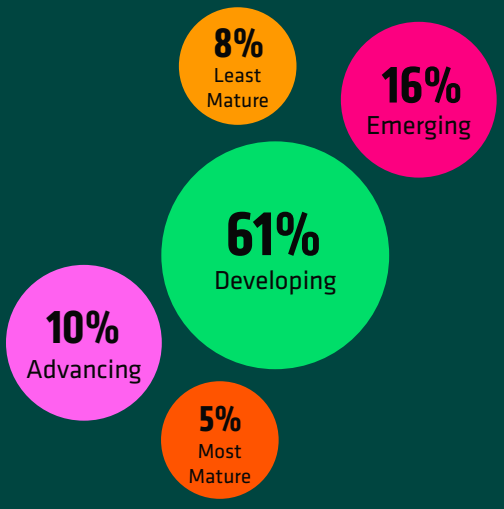
Identify and prioritize systems for backup

Midsize organizations are using data discovery and classification more strategically across compliance, response, and recovery. Nearly two-thirds address privacy and security violations, while over half use classification to guide compliance during an attack. More than half also define materiality before an incident and prioritize backups based on risks. Mature cyber resilience transforms classification into a systematic approach that optimizes data risk posture and informs protection, response, and recovery.

## A CLEARER PICTURE OF RESILIENCE MATURITY

When scored collectively, respondents' answers served as a high-level barometer of cyber resilience maturity, revealing clear patterns in how midsize organizations are building – or struggling to build – resilience in practice. While the majority fall into the developing stage, only 5% demonstrate the most mature, integrated capabilities that define risk-ready organizations.

### THE CYBER RESILIENCE MATURITY CURVE




**Least Mature (8%):** Backups, policies, and security safeguards are largely absent or inconsistent. MFA and admin controls are rarely enforced, recovery often lacks isolation, and compliance or materiality assessments are typically overlooked.

**Emerging (16%):** Some resilience practices are in place, but inconsistently. Organizations may back up sensitive data, apply global policies, or use MFA, but rarely in combination. Threat intelligence and compliance efforts exist yet remain immature and fragmented.

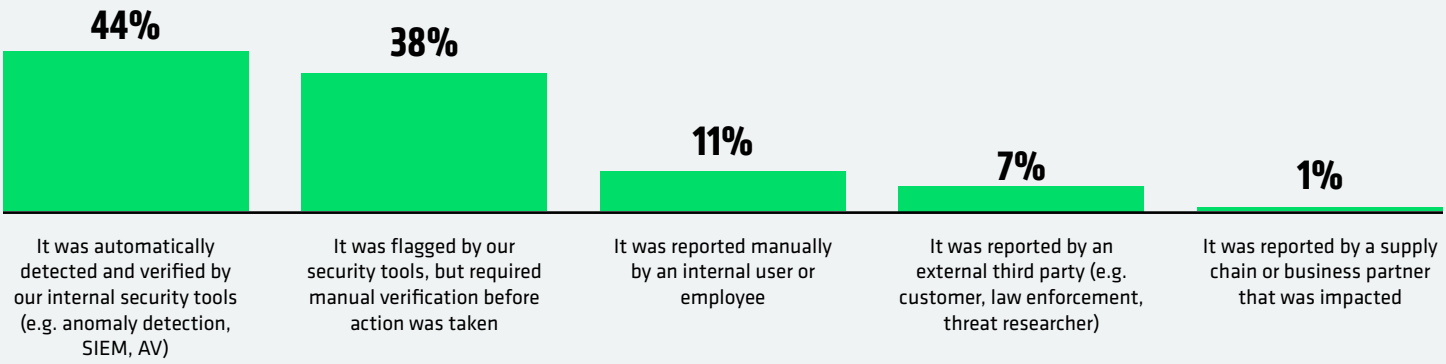
**Developing (61%):** Core practices such as backups, admin controls, and threat intelligence are more common, though still uneven. Recovery environments, compliance checks, and security gap remediation are applied sporadically, leaving resilience efforts partially effective.

**Advancing (10%):** Most key practices are consistently enforced, including global backup policies, admin approvals, and remediation before recovery. Threat intelligence is used but not fully optimized, and some gaps remain around isolated recovery and full compliance coverage.

**Most Mature (5%):** Resilience is systemic and comprehensive. Sensitive data is backed up globally, MFA and admin controls are standard, threat intelligence is maximized, recovery is secured through remediation, and compliance safeguards are consistently met.

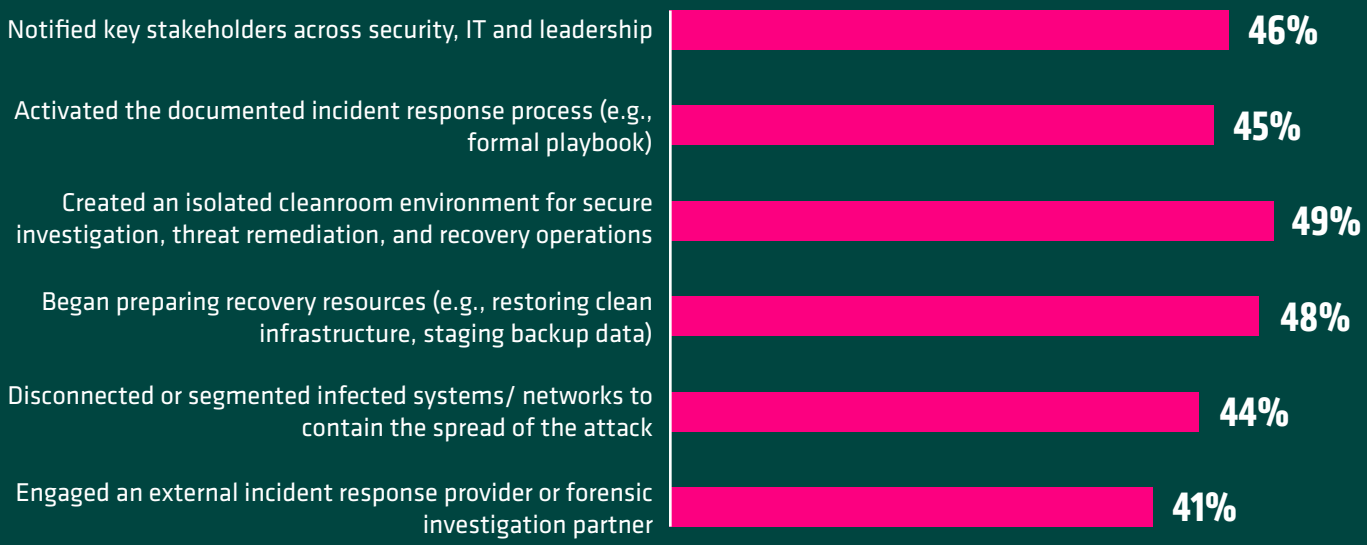
# RESILIENCE UNDER FIRE

## HOW TEAMS IDENTIFIED THE ATTACK



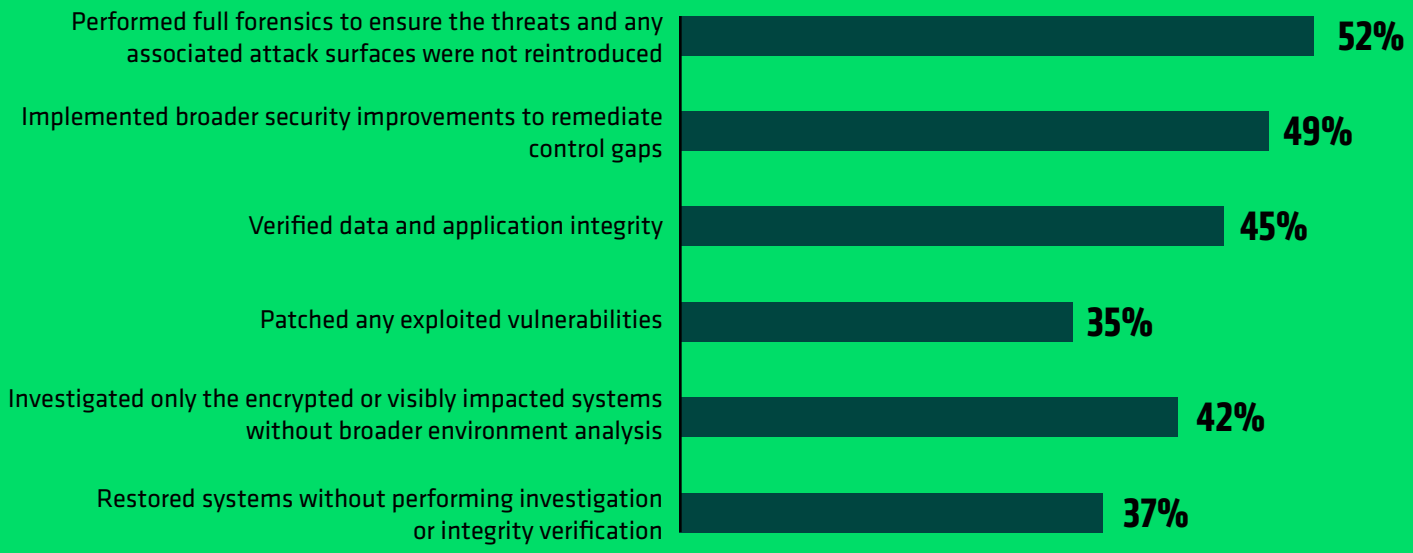

In the event of a cyberattack, most midsize organizations detect incidents internally with the largest share identified automatically and verified by security tools. Many others are flagged by tools but require manual verification before action is taken. Far fewer incidents are reported by employees or external parties. Detection is largely tool-driven, though human validation still plays an important role.

## ACTIONS TEAMS TOOK AFTER CONFIRMING THE ATTACK



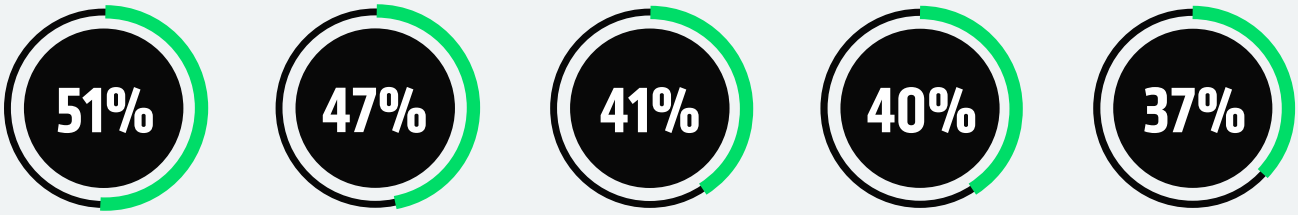

After confirming an attack, midsize organizations took a range of actions to contain the threat and begin recovery. Similar shares began preparing recovery resources, created isolated cleanroom environments, notified key stakeholders, disconnected infected systems, and activated response playbooks. Slightly fewer engaged external incident response partners. These patterns suggest response efforts are broadly adopted but not yet fully standardized across critical actions.

## STEPS TAKEN BEFORE BRINGING SYSTEMS AND DATA BACK ONLINE




Before bringing systems and data back online, midsize organizations employed a mix of forensic and remediation measures. About half performed full forensics, implemented broader security improvements, or verified data and application integrity, while similar numbers focused only on visibly impacted systems. Smaller shares patched exploited vulnerabilities or restored systems without investigation or verification. These gaps may increase the risk of reinfection or residual exposure.

## CHALLENGES TEAMS FACED DURING THE ATTACK




Inability to communicate or coordinate within our team due to critical systems being down (e.g. email, collaborative applications, ticketing)

Pressure from leadership to restore systems before the attack was remediated

Security tools were evaded, and backups were attacked

We recovered, but were later reinfected because threats weren't fully eradicated

Lack of access to clean, validated recovery points

Teams faced a range of operational and technical challenges during the attack. About half struggled to communicate while systems were down or felt pressure to restore systems before remediation was complete. Teams also reported security tool evasion, attacked backups, reinfection after recovery, or lack of access to clean recovery points. These challenges highlight gaps in preparedness that can complicate response and prolong disruption.

## WHERE RESILIENCE INVESTMENT STILL FALLS SHORT

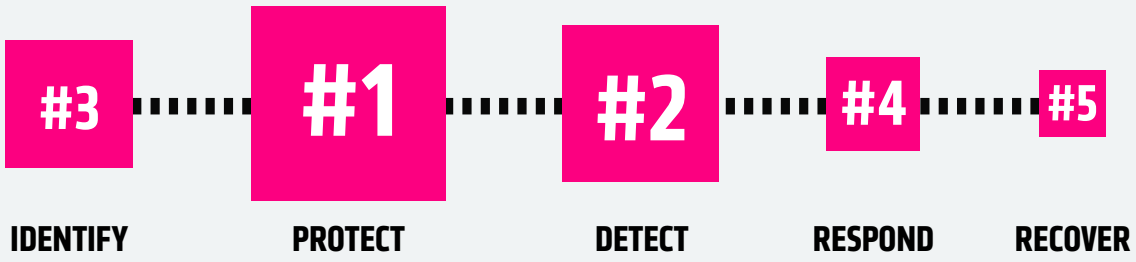
Even well-prepared organizations struggle to sustain resilience once an attack unfolds. As operational pressure mounts, coordination gaps, incomplete remediation, and reinfection risks expose how fragile recovery can be without unified processes and continuous assurance.

These patterns mirror how midsize organizations are allocating their cyber resilience budgets today. We asked respondents how they proportion spending across the five core functions of the NIST Cybersecurity Framework—Identify, Protect, Detect, Respond, and Recover.

Most continue to invest heavily in prevention, protection, and detection, while comparatively less funding supports response and verified recovery. The result is a maturity curve still weighted toward defense rather than restoration, highlighting an untapped opportunity to strengthen resilience where it matters most: after the attack.

### NIST CYBERSECURITY FRAMEWORK.

Box size shows highest to lowest proportion of cyber resilience investments




## AI AND AUTOMATION EMERGE AS RESILIENCE MULTIPLIERS

The results also show that midsize organizations view AI as a powerful enabler of cyber resilience, particularly in improving detection speed and response precision. Nearly all respondents rated tools such as anomaly detection, user behavior analytics, and AI-driven threat investigation and response as effective in strengthening their security posture.

Even newer GenAI-based assistants, capable of natural language threat queries and contextual analysis, are gaining traction as a way to simplify and accelerate decision-making. Fifty-six percent of midsize organizations said one of the biggest lessons learned after a cyberattack was the need for greater automation across detection, response, and recovery. This reflects the growing demand for integrated automation and orchestration platforms, where AI acts as a force multiplier, driving greater efficiency, consistency, and effectiveness across these processes.

When looking ahead, most expect AI to play an increasingly strategic role in cyber defence by the end of 2026. Fifty-six percent anticipate AI will support human decision-making, enhancing analysis and recommendations, with humans remaining in control of final actions. Thirty-seven percent expect AI to become central to detection and response, even making some autonomous decisions. This signals a clear trajectory: AI is evolving from an assistant to an operational cornerstone of cyber resilience, poised to enhance speed, precision, and confidence across detection, response, and recovery.

# THE FUTURE OF RESILIENCE STARTS NOW

While midsize organizations are making measurable progress in cyber resilience, many still have room to improve their response, recovery, and validation of readiness after an attack. Cyber resilience represents a massive competitive advantage. The future belongs to organizations that invest in the people, products, and processes to recover faster, maintain customer trust, and keep business moving when others can't. When disruption is virtually inevitable, resilience isn't just protection; it's performance.

Build resilience before crisis strikes:

- Learn about Cohesity's cyber resilience solutions for midsize organizations
- Assess your cyber resilience maturity with this resilience scorecard
- Level up with a five-step cyber resilience action plan

## METHODOLOGY

COHESITY

Cohesity commissioned Vanson Bourne to survey 3,200 IT and Security decision-makers in September 2025, forming the basis of these findings. Respondents represent organisations in the US (500), Brazil (200), UK (400), Germany (400), France (400), UAE/Saudi Arabia (100), Australia (200), South Korea (200), Japan (400), India (200), and Singapore (200). The organisations had 1,000 or more employees and came from a range of public and private sectors, with a focus on financial services, public sector, and healthcare.



COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000049-001 EN 11-2025